# NASA Policy Directive

**NPD 2540.1I**
Effective Date: August 19, 2019
Expiration Date: August 19, 2024

**COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES**

Printable Format (PDF)

## Subject: Acceptable Use of Government Office Property Including Information Technology

**Responsible Office: Office of the Chief Information Officer**

## SPECIAL ATTENTION: ONLY USE

## NID 2540.138 Acceptable Use of Government Office Property Including Information Technology.

### 1. POLICY

a. It is NASA's policy to permit limited acceptable personal use of Government furnished property (GFP) and information technology (IT) services for non-government purposes, when such use involves minimal additional expense to the Government, does not overburden any of the Agency's IT resources, and when access to these IT resources does not interfere with official Government business. The intent is to provide a professional and supportive work environment while meeting taxpayer expectations that tax dollars be spent wisely. Acceptable personal use incurs only minimal additional expense to the Government in areas such as: communications infrastructure costs; use of consumables in limited amounts; general wear and tear on property; minimal data storage on storage devices; and, minimal network impacts, keeping e-mail message sizes (including attachments) within NASA specified size guidelines.

b. It is NASA policy to permit limited acceptable personal use of GFP and IT services to individuals during non-duty time for periods of reasonable duration and frequency of use such as during the lunch break and when use does not adversely affect the performance of official duties, result in the loss of an individual's productivity, or interfere with the mission of NASA.

c. NASA policy requires that computer systems and networks are not used for downloading illegal, inappropriate, or unauthorized content and untrusted, unapproved, or malicious software applications.

d. This NASA Policy Directive (NPD) in no way limits Agency employees' and contractors' use of GFP and IT services for official Government activities, or limits the rights any employee may have under Government- wide statute or regulation.

e. As a matter of NASA policy, individuals have no expectation of privacy while using any NASA GFP and IT resources at any time, including (but not limited to) accessing the Internet, proxy avoidance server, or e-mail. Individuals should be aware that their rights to privacy do not change even during limited periods of personal use. To the extent that individuals wish their private activities remain private, they should avoid using NASA GFP and IT resources.

f. Compliance with this NPD is mandatory. Non-compliance or unauthorized or improper use of NASA GFP and IT may result in the suspension or revocation of access to NASA IT, and disciplinary action, as well as civil and criminal penalties.

### 2. APPLICABILITY

a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory, a Federally Funded Research

and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. In this NPD, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

c. This NPD applies to employee acceptable personal use of GFP, non-GFP, personally owned devices when connected to NASA networks or IT resources or containing NASA data, and IT services, whether owned or otherwise provided by NASA Headquarters and NASA Centers, including Component Facilities. Federal Acquisition Regulation, Government Property, 48 CFR pt. 45; NASA FAR Supplement, Government Property, 48 CFR 1800, pt. 1845; and the terms and conditions of individual contracts provide additional policies and procedures for contractor-accountable, NASA-owned property and for Center-accountable, NASA-owned property.

d. In this NPD, all document citations are presumed to be the latest version unless otherwise noted.

## 3. AUTHORITY

a. Federal Information Security Modernization Act of 2014, 44 U.S.C. §3554.

b. The National Aeronautics and Space Act, 51 U.S.C. §20113.

c. Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR §2635.101(b)(9) and 704A.

d. Federal Information Processing Standards Publication (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems.

## 4. APPLICABLE DOCUMENTS AND FORMS

a. NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy.

b. NASA Procedural Requirements (NPR) 1382.1, NASA Privacy Procedural Requirements.

## 5. RESPONSIBILITY

a. The Office of the Chief Information Officer (OCIO) is responsible for development, implementation, and management of this NPD, and ensuring this policy is widely disseminated to all NASA employees and contractors.

b. Each Center Director and the Executive Director for Headquarters Operations is responsible for developing and promulgating procedures for ensuring that NASA employees and contractors are aware of proper personal use of GFP, non-GFP, personally owned devices when connecting to NASA system or data, NASA systems, and NASA IT services; and developing cost- effective controls for monitoring or preventing abnormal or inappropriate use. Controls to be considered for GFP include blocking of inappropriate Web sites and phone numbers, flagging abnormal long distance or phone charges, and monitoring network traffic for suspicious traffic or inappropriate use.

c. Supervisors shall:

(1) Promote the appropriate use of Government office property and services, including IT, and pursuing sanctions for misuse, including potential disciplinary action.

(2) Permit a reasonable period of time for personal use of social media technologies by employees and contractors during non-duty time or while using Government property.

d. Visitors and interns will be allowed, if explicitly authorized by the Information System Owner (ISO), to use Government office property, U.S. Government limited access data/information, and IT services. The ISO will ensure visitors and interns are knowledgeable of Federal and Agency policy before use of the property, U.S. Government limited access data/information, or IT.

e. Employees and contractors are responsible for knowing Federal and NASA requirements and complying with personal use privileges of GFP and IT services as outlined herein and in Attachment C (Specific Provisions) to this directive. Employees and contractors will ensure that their personal use of GFP and IT services does not give rise to an appearance that they are acting in an official capacity or that NASA endorses or sanctions any personal activities and the personal use is otherwise consistent with Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR pt. 2635.

(1) When using Government furnished property and during duty hours, NASA employees and contractors bear the responsibility of using social media tools in a responsible, safe, and judicious manner, whether in an official capacity

or through personal use, and to protect mission objectives, information assets, program integrity, data, and NASA's reputation.

(2) NASA employees and contractors will distinguish between official and personal communications to ensure that all official communications are identified and conducted in conformance with applicable law, regulation, and policy.

(3) NASA employees and contractors shall conduct themselves professionally in the workplace and not use Government property for activities that are inappropriate or illegal.

(4) NASA employees and contractors are not permitted or authorized to download, copy, or install unapproved or unauthorized software applications or data programs onto NASA-provided or NASA-approved and authorized devices, or NASA IT services or systems such as screen savers, computer games, test or demo software, or "push" technology applications. Other activities such as peer-to-peer (P2P) file sharing, online gaming or gambling, and cryptocurrency-mining by NASA employees and contractors on NASA-provided or NASA-approved and authorized devices, or with NASA IT services or systems, are also prohibited. Viewing or accessing the following types of Web sites are also prohibited:

(a) Pornographic, sexually explicit, or sexually oriented materials.

(b) Personal services Web sites, such as dating services where users register using NASA credentials and create an appearance that user is acting in an official capacity or that NASA endorses/sanctions the activity.

(c) Hacker sites (sites which expose NASA to unacceptable security risk) regardless of the known or potential security risks or lack thereof.

(d) Proxy avoidance sites (or similar capabilities) such as 3Proxy, Unblockme, and Proxite.

(5) Users shall only use the NASA guest network for non-NASA business and access the network utilizing non-NASA property.

(6) Users shall not connect unauthorized non-NASA devices to GFP via Universal Serial Bus (USB), Bluetooth, or other connection methods.

(7) When GFP IT is taken out of the workplace (i.e., telework, offsite business meetings, conferences), the employee or contractor will ensure that the property is configured in accordance with Agency policy, remains in their custody, is handled and maintained properly, and is returned in good condition. In the event that the GFP is lost, stolen, or damaged, the employee or contractor shall notify their supervisor, the NASA Security Operations Center (SOC) at soc@nasa.gov or 1-877-NASASEC (1- 877-627-2732), and Center Physical Security as soon as possible after the occurrence of an incident.

(8) Employees and contractors shall not interfere with official business or violate applicable laws through limited acceptable personal use of NASA GFP and IT services.

(9) Employees and contractors shall involve only minimal additional expense to the Government through limited acceptable personal use of NASA GFP and IT services.

(10) The privilege to use NASA GFP and IT services for non-government purposes may be revoked or limited at any time by Federal or Agency officials. NASA Centers and contractors may invoke more stringent policies or implementation guidance.

f. Contracting officers are responsible for:

(1) Ensuring that contractors are informed of appropriate uses of Government IT resources, approved/authorized non-GFP, and personally owned devices as a part of their introductory IT security training, orientation, or the initial implementation of this policy as part of the NASA contract; and is addressed in the IT Security Plan and IT Security Management Plans.

(2) Ensuring contractors who process, store, or transmit NASA information on approved/authorized non-GFP or personally owned devices, IT equipment, software, and media do so only when the contract under which they perform specifically establishes terms and conditions for such use (and that appropriate approvals have been obtained), and the contractor otherwise meets and complies with NASA security standards.

## 6. DELEGATION OF AUTHORITY

None.

## 7. MEASUREMENT/VERIFICATION

Information System Owners may access any electronic communications made via NASA GFP and/or IT resources and employ monitoring tools to detect improper use. ISOs or their designees determine, implement, ensure, and document compliance by applying a verification approach that is tailored to meet the requirements of this NPD. The Office of Protective Services (OPS) conducts functional reviews, spot checks, and inspections to review compliance and implementation. The ISO employs enterprise tools on their systems to detect unauthorized access.

## 8. CANCELLATION

NPD 2540.1H, Personal Use of Government Office Equipment Including Information Technology, February 24, 2016.

## /s/ Jim Bridenstine
## Administrator

---

## ATTACHMENT A. DEFINITIONS

"Property" means a tangible asset, end item, or nonexpendable property that is functionally complete, not intended for sale, does not lose its identity, or become a component part of another item when put into use. Property is not intended to be destroyed during an experiment and has a useful life of two years or more.

"Government furnished property" means property owned or leased by the Government. Government office property is property in the possession of, or directly acquired by, the Government and can be subsequently furnished to the contractor for performance of a contract.

Government furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. (Federal Acquisition Regulation, Part 45.101) Government furnished property includes, but is not limited to: computers and related peripheral property and software, library resources, research or reference services (e.g., online journals), telephones and wireless communications devices (e.g., cell phones, smartphones, pagers), personal electronic devices (e.g., calculators, music players, global positioning system devices, book readers), facsimile machines, photocopiers, office supplies, Government guest networks, network access (e.g., Internet, wireless, cellular), e-mail, and licenses (e.g., software licenses.) This also includes property provided for use while in official travel status and for a telework or other alternative work space arrangement.

"Information System Owner," per NPR 1382.1, NASA Privacy Procedural Requirements, means the principal advisor to the Center Information Security Officer (CISO) on matters pertaining to specific information systems.

"Information Technology," per Definitions, 40 U.S.C. § 11101(6) is:

Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a Federal contractor incidental to a Federal contract. For additional guidance/clarification on meaning or scope of IT, please refer to the definition for "Information System" which is a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"NASA Information," per NPD 2810.1, NASA Information Security Policy, means any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for or is under the control of NASA.

"Personally owned device" includes but is not limited to any device such as a phone, tablet, laptop, personal computer, Internet of Things device, or wearable technology that does not have a valid Authorization to Operate (ATO) from a NASA Authorizing Official (AO).

"Personal use" means other than for official Government business.

"Peer-to-Peer file sharing," as defined in OMB M-04-26, Personal Use Policies and "File Sharing" Technology, refers to any software or system allowing individual users of the Internet to connect to each other and trade files.

"Privilege" means, in the context of this policy, that NASA is extending the opportunity to its employees and contractors to use GFP for limited personal use to create a more supportive work environment. Employees and contractors have no inherent right to personal use or ownership of GFP. The personal use privilege does not extend to modifying GFP, including modifications such as loading personal software or making configuration changes, or other changes that are inconsistent with Agency policy.

"Social media technologies" include, but are not limited to, wikis, blogs, mash-ups, Web feeds (e.g., Really Simple Syndication and Rich Site Summary (RSS) feeds), social networking sites (e.g., Facebook), microblogging (e.g., Twitter), and Web-based forums.

## ATTACHMENT B. ACRONYMS

CFR Code of Federal Regulations

CIO Chief Information Officer

CISO Center Information Security Officer

FAR Federal Acquisition Regulations

FFRDC Federally Funded Research and Development Center

FIPS Federal Information Processing Standards Publication

GFP Government Furnished Property

ISO Information System Owner

IT Information Technology

ITS Information Technology Security

NASA National Aeronautics and Space Administration

NPD NASA Policy Directive

NPR NASA Procedural Requirement

OMB Office of Management and Budget

P2P Peer-to-Peer

SOC Security Operations Center

U.S.C. United States Code

## ATTACHMENT C. SPECIFIC PROVISIONS

C.1 Employees are permitted limited personal use of GFP and IT services to the extent that such personal use does not interfere with official duties or result in a loss of productivity and for contractors only to the extent specified or referenced in the appropriate contracts. Employees and contractors are only authorized to use office property and services for personal use if they are first authorized to use the property for official business. NASA is not required to supply property if the property is not required for the employee or contractor to perform official business. Moreover, personal use can incur only minimal additional expense to the Government in areas such as:

C.1.1 Communications infrastructure costs such as, but not limited to, telephone or data charges, Internet connectivity, and telecommunications traffic.

C.1.2 Consumables such as, but not limited to, paper, ink, and toner.

C.1.3 Wear and tear on property such as, but not limited to, copiers and printers.

C.1.4 Impacts to network bandwidth such as, but not limited to, e-mail message sizes, e-mails with attachments, text messaging, music streaming, and personal use of social media (e.g., Twitter, Facebook, YouTube).

C.2 Inappropriate Personal Use - Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using GFP and IT services for activities that are inappropriate. Misuse or

inappropriate use of GFP and IT services includes, but is not limited to:

C.2.1 Any personal use that violates applicable law, regulation, Federal or Agency policies, or procedural requirements.

C.2.2 Any personal use that could cause unnecessary congestion, delay, or disruption of service to any Government system or component.

C.2.3 Using a Government system as a staging ground or platform to gain unauthorized access to other systems.

C.2.4 The creation, copying, transmission, or retransmission of unauthorized mass mailings, regardless of subject matter.

C.2.5 Activities inconsistent with the Standards of Ethical Conduct for Employees of the Executive Branch 5 CFR pt. §2635.

C.2.6 Accessing, sharing, posting, storing, or copying material that is inappropriate or offensive based on race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, gender identity, or status as a parent.

C.2.7 Creating, searching/downloading, viewing, storing, copying, or transmitting materials describing or depicting sexually explicit conduct, or other sexually explicit or sexually oriented materials.

C.2.8 Use for commercial purposes, "for profit" activities, or in support of outside employment or business activity such as a personal business, or assisting friends, relatives, or others in such activities (e.g., consulting for pay, sales, or administration of business transactions, and sale of goods or services).

C.2.9 Engaging, in a personal or private capacity, in any outside fund- raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).

C.2.10 Publicly communicating Agency information, including Agency policy, project, or program information and other critical data, that does not concern a protected disclosure under Government Organizations and Employees, 5 U.S.C. Title 5, or that has not been authorized for release. This includes uses that could create the perception that the communication was made on behalf of the Agency or the Office of the Administrator if the communication has not been authorized by the Office of Communications. Authorized public communications of Agency information are subject to Release of Information to News and Information Media, 14 CFR, pt. 1213, and applicable Agency policies.

C.2.11 Any use that could generate more than minimal additional expense to the Government.

C.2.12 The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy, copyrighted, trademarked information, or material with other intellectual property rights (such as literature, music, and videos beyond fair use), proprietary data, or export-controlled software or data.

C.2.13 Participate in P2P file sharing activities.

C.2.14 Overriding or defeating a security feature of a Government system (e.g., installing unapproved software).

C.3 Privacy Expectations - NASA employees and contractors do not have a right to expect privacy while using Government office property or IT services at any time, including accessing the Internet and using e-mail. Employees and contractors are advised that the Government maintains call detail and network access records to monitor telephone activity and Internet access and employs monitoring tools to track system performance and improper use. To the extent that employees and contractors wish their private activities to remain private, they should avoid personal use of GFP and IT services. By using GFP, employees and contractors consent to disclosing the contents of any files or information maintained on or passed through the property. Any use of Government communication resources is made with the understanding that such use is subject to Government surveillance and inspection, is not private, and is not anonymous. This includes personal property (e.g., tablets, smartphones) that connect to Government networks and services.

C.4 Sanctions for Misuse - Unauthorized or improper use of GFP and IT services could result in loss of use or limitations on use of property, disciplinary or adverse personnel actions, criminal penalties, and/or employees/contractors being held financially liable for the cost of improper use.

## ATTACHMENT D. REFERENCES

D.1 Government Organizations and Employees, 5 U.S.C. Title 5.

D.2 The Hatch Act, 5 U.S.C. § 7323.

D.3 Definitions, 40 U.S.C. § 11101(6).

D.4 Principles of Ethical Conduct for Government Officers and Employees. Executive Order (EO) 12674 of April 12, 1989, as amended by EO 12731 of October 17, 1990.

D.5 Federal Information Technology, E.O. 13011 of July 16, 1996, as amended by E.O. 13284 of January 23, 2003, and E.O. 13286 of February 28, 2003.

D.6 Release of Information to News and Information Media, 14 CFR, pt. 1213.

D.7 Federal Acquisition Regulation, Government Property, 48 CFR pt. 45.

D.8 NASA FAR Supplement, Government Property, 48 CFR 1800, pt. 1845.

D.9 OMB M-04-26, Personal Use Policies and "File Sharing" Technology.

D.10 OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

D.11 OMB M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements.

D.12 NPD 1900.9, Ethics Program Management.

D.13 NPD 2810.1, NASA Information Security Policy.

D.14 NPR 1900.3, Ethics Program Management.

D.15 NPR 2810.1, Security of Information Technology.

D.16 NPR 3600.2, NASA Telework Program.

D.17 NPR 4200.1, NASA Equipment Management Procedural Requirements.

D.18 NASA Information Technology Security Handbook (ITS-HBK) 2810.07-01, Configuration Management.

D.19 ITS-HBK-2810.15-01, Access Control.

D.20 ITS-HBK-2810.17-01, Identification and Authentication.

D.21 NASA ITS-SOP 2810.01A, Collection of Electronic Data.

**(URL for Graphic)**

None.

**DISTRIBUTION:**
**NODIS**




**This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.**